Claims:

1. A method for authentication in a communication device in which identification data is stored in connection with the communication device, **wherein** the authentication is divided in at least two steps of authentication, wherein in the first authentication step, at least one security inquiry containing identification data of the communication device is transmitted to the communication device, said identification data contained in the security inquiry is examined in the communication device to find out if the identification data matches with the identification data stored in the communication device, wherein if the comparison shows that the identification data do not match, a time control is started, wherein the processing of the next security inquiry message transmitted to the communication device is started after the expiry of said time control in the communication device, and that the second authentication step is only taken if the comparison shows that said identification data match.

2. The method according to claim 1, in which the communication device is logged in a communication network, **wherein** the authentication is performed at least in connection with the logging of the communication device in the communication network.

3. The method according to claim 1, **wherein** said time control is delayed an the increase in the number of such security inquiries in which the identification data do not match with the identification data stored in the communication device.

4. The method according to claim 1, **wherein** the communication device used is a wireless communication device.

5. The method according to claim 4, **wherein** a SIM card is used for storing the identification data in the wireless communication device.

6. A communication device comprising means for storing identification data, **wherein** the means for storing identification data comprise means for performing the authentication in at least two steps of

authentication, wherein the communication device comprises means for receiving at least one security inquiry containing identification data of the communication device transmitted to the communication device in the first authentication step; means for examining said identification data contained in the security inquiry to find out if the identification data matches with the identification data stored in the communication device; means for starting a time control if the comparison shows that the identification data do not match; and means for starting the processing of the next security inquiry message transmitted to the communication device after the finish of said time control in the communication device; and that the second authentication step is arranged to be taken only if the comparison shows that said identification data match.

7. The communication device according to claim 6, **wherein** the means for starting the time control comprise means for extending the time control period in the case of an increase in the number of such security inquiries in which the identification data do not match with the identification data stored in the communication device.

8. The communication device according to claim 6, **wherein** the communication device is a wireless communication device.

9. The communication device according to claim 8, **wherein** the means for storing identification data comprise a SIM card.

10. A communication system comprising at least one communication network and a communication device comprising means for storing identification data, **wherein** the means for storing identification data comprise means for performing the authentication in at least two steps of authentication, wherein the communication device comprises means for receiving at least one security inquiry containing identification data of the communication device transmitted to the communication device in the first authentication step; means for examining said identification data contained in the security inquiry to find out if the identification data matches with the identification data stored in the communication device; means for starting a time control if the comparison shows that

the identification data do not match; and means for starting the processing of the next security inquiry message transmitted to the communication device after the finish of said time control in the communication device; and that the second authentication step is arranged to be taken only if the comparison shows that said identification data match.

11. The communication system according to claim 10, comprising means for logging of the communication device in a communication network, **wherein** the authentication is arranged to be performed at least in connection with the login of the communication device in the communication network.

12. The communication system according to claim 10, **wherein** the communication network comprises at least one mobile communication network, and that the communication device is a wireless communication device.

13. An identification card comprising means for storing identification data, **wherein** the means for storing identification data comprise means for performing the authentication in at least two steps of authentication, wherein the identification card comprises means for receiving at least a security inquiry in the first authentication step, the security inquiry containing identification data of a communication device; means for examining said identification data contained in the security inquiry to find out if the identification data matches with the identification data stored in the communication device; means for starting a time control if the comparison shows that the identification data do not match; and means for starting the processing of the next security inquiry message transmitted to the communication device after the expiry of said time control in the communication device; and that the second authentication step is arranged to be taken only if the comparison shows that said identification data match.